UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCION DEL TITULO DE:

INGENIERIA EN SISTEMAS.

TEMA:

ANALISIS DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS) OPEN SOURCE Y SOFTWARE PROPIETARIO.

EGRESADA:

JENNY ISABEL CASTILLO MENDOZA

TUTOR:

JOSÉ TEODORO MEJÍA VITERI

RESUMEN

En la actualidad es importante mantener las redes seguras, las amenazas están en constante evolución, los usuarios y/o empresas se esfuerzan en contener y evitar ataques que pueden poner en peligro la información, es por ello que existen diferentes herramientas como lo son los Sistemas de Detección de Intrusos (IDS) que permiten detectar accesos no autorizados o ataques realizados a un sistema o una red.

Este caso de estudio proporciona una comparación entre los diferentes sistemas de detección de intrusos de plataforma Open Source: Snort y Suricata, y de Software propietario: Nessus y Atomic OSSEC. Es importante que los usuarios y/o empresas conozcan más sobre las diferentes características y funcionalidades de los sistemas de detección de intrusos

A pesar de sus diferencias tienen algo en común que es detectar intrusiones, por eso son herramientas importantes para la seguridad, al querer implementar un IDS es importante que los usuarios y empresas tengan en cuenta sobre las características de los sistemas de detección de intrusos, porque de esa manera puede conocer que sistema puede usar de acuerdo a sus requerimientos.

Palabras claves: Sistema de detección de intrusos, Open Source, Software propietario, ataques, amenazas, información.

ABSTRACT

Nowadays it is important to keep networks secure, threats are constantly evolving, users and/or companies strive to contain and prevent attacks that can endanger information, which is why there are different tools such as Intrusion Detection Systems (IDS) that allow the detection of unauthorized access or attacks made to a system or a network.

This case study provides a comparison between the different open source platform intrusion detection systems: Snort and Suricata, and proprietary software: Nessus and Atomic OSSEC. It is important that the users and/ or companies know more about the different feature and functionalities of the different systems.

Despite their differences, they have something in common, which is to detect intrusions, which is why they are important tools for security. When wanting to implement an IDS, it is important that users and companies take into account the characteristics of intrusion detection systems, because that way you can know which system you can use according to your requirements.

Keywords: Intrusion detection System, Open Source, Proprietary Software, attacks, threats, information.

INTRODUCCION

En la actualidad es importante mantener seguras las redes, los usuarios y/o empresas se esfuerzan en contener y evitar ataques que puedan poner en peligro la información, es por ello que existen diferentes herramientas para evitar estos ataques y es importante conocer sus características, funcionalidades y ventajas de los sistemas de detección de intrusos porque estos permiten detectar accesos no autorizados.

Las amenazas están en constante evolución, los usuarios y empresas enfrentan riesgos informáticos como virus, troyanos, gusanos, malware y amenazas nuevas y desconocidas que son difíciles de detectar a simple vista y sobre todo prevenir porque no se sabría en que momento se podría enfrentar a un ataque informático, mantener la red a salvo de intrusiones es una de las partes vitales de la administración y seguridad del sistema, redes y sobre todo de la información, pero es indispensable conocer las características de los sistemas de detección de intrusos.

Los ciberataques no dejan de producirse y es necesario que los usuarios y empresas implanten diferentes medidas y es ahí cuando surge el problema de no conocer qué tipo de sistema de detección de intruso utilizar, sea porque es gratuito o por su costo, por su funcionamiento o por sus diferentes características y al buscar información no se encuentra documentada.

El presente caso de estudio tiene como objetivo conocer de forma comparativa las características principales de los diferentes tipos de sistemas de detección de intrusos (IDS) Open Source y Software propietario que ayuden a la seguridad del sistema.

Este documento se lo desarrollo utilizando la línea de investigación de sistemas de información y comunicación, emprendimiento e innovación con su referente en la sub línea de investigación en Redes y tecnología inteligentes de software y hardware.

La metodología a utilizar es de la investigación descriptiva porque de esta manera permite identificar las diferentes características de los sistemas de detección de intrusos, al utilizar esta metodología facilito la obtención de información, la investigación se elaboró bajo el planteamiento del enfoque cualitativo porque este método permite realizar un análisis y comparación de la información que se obtuvo a lo largo de la investigación. La técnica de recolección de datos fue mediante el análisis documental y bibliográfico porque permite reunir información de diferentes fuentes.

DESARROLLO

Uno de los mecanismos de defensa más usados para reducir el riesgo de ataques dirigidos hacia los bienes informáticos han sido los sistemas de detección de intrusos o IDS (Intrusion Detection Systems). Los Sistemas de Detección de Intrusos constituyen una herramienta importante para la seguridad además que es un elemento que analiza toda la información que circula por una red de datos e identifica posibles ataques. En el momento que intenten realizar un ataque el sistema reaccionara informando al administrador y cerrara las puertas a los posibles intrusos reconfigurando elementos de la red como firewalls y routers (Lopez J. G., 2015).

La cantidad de intentos de accesos no autorizados a la información que existe en internet ha ido creciendo durante estos últimos años, en la mayoría de las instituciones u organizaciones estos intentos pueden ser o no detectados debido a que al momento no han implementado mecanismos de seguridad en su infraestructura tecnológica. Muchas empresas u organizaciones normalmente por motivos de costo han migrado información clave a internet exponiéndola a peligros por eso estos sistemas están continuamente supervisando los componentes de la red y las computadoras o intrusos que están intentando entrar de forma ilegal

Los sistemas de detección de intrusos suele están formados por: los sensores, los analizadores y la interfaz de usuario, la responsabilidad de los sensores es de coleccionar datos de interés y enviar esta información a los analizadores. Los analizadores determinan si

ha ocurrido o está ocurriendo una intrusión y por último la interfaz de usuario proporciona pruebas y el tipo de intrusión detectada y muchos de los casos, proponen o ejecutan un grupo de medidas que actúan sobre ellas. (Miranda, 2014)

Clasificación de los Sistemas de Detección de Intrusos

Los sistemas de detección de intrusos pueden clasificarse en diferentes tipos, en función del sistema que monitorea y en función de cómo se implementan a continuación de describe cada uno de ellos:

Sistema de Detección de Intrusos de red (NIDS).

El sistema de detección de intruso basado en la red o NIDS generalmente se implementa o coloca en puntos estratégicos de la red, destinado a cubrir aquellos lugares donde el tráfico es más vulnerable a los ataques. (Briceño, 2021)En general se aplica a subredes completas e intenta hacer coincidir el tráfico que pasa con una biblioteca de ataques conocidos. Además que examina de forma pasiva el tráfico de red que llega a través de los puntos de la red en la que se implementa. El software del sistema de detección de intrusos basado en la red analiza una gran cantidad de trafico de red, lo que significa que a veces tienen poca especificidad esto significa que a veces pueden perder un ataque o no detectar algo que sucede en el trafico encriptado.

Sistema de Detección de Intrusos en Host (HIDS).

Un sistema de detección de intrusos basados en host o HIDS se ejecuta en todas las computadoras o dispositivos en la red con acceso directo tanto a internet como a la red interna de la empresa u organización. Un HIDS tiene la ventaja sobre un NIDS y es que puede detectar paquetes de red anómalos malicioso que un NIDS no ha podido detectar. También

puede identificar el tráfico malicioso que se origina en el propio host, como cuando el host ha sido infectado con malware y está intentando propagarse a otros sistemas. (Zorrilla, 2020)

Sistema de Detección de Intrusos basado en firmas (SIDS).

Un sistema de detección de intrusos basado en firmas monitoriza todos los paquetes que atraviesan la red y los compara con una base de datos de firmas de ataque o atributos de amenazas maliciosas conocidas al igual que el software antivirus. (Atico, 2021) Este tipo de sistema de detección de intruso se centra en la búsqueda de una "firma", patrones o una identidad conocida, de una intrusión o evento de intrusión específico.

Sistema de Detección de Intrusos basado en anomalías (SIDA).

Un sistema de detección de intrusiones basado en anomalías monitoriza el tráfico de la red y lo compara con una línea de base establecida para determinar lo que se considera normal para la red con respecto al ancho de banda, protocolos, puertos y otros dispositivos. Este tipo de sistema a menudo utiliza el aprendizaje automático para establecer una línea de base y una política de seguridad que la acompañe.

Al detectar amenazas utilizando un modelo amplio en lugar de firmas y atributos específicos, el método de detección basado en anomalías busca los tipos de ataques desconocidos y mejora las limitaciones de los métodos basados en firmas especialmente en la detección de nuevas amenazas. Además los sistemas de detección de intrusos basados en anomalías suponen que el comportamiento de la red siempre es predecible y puede ser simple distinguir en buen tráfico del mal.

Funcionamiento

El funcionamiento de un Sistema de detección de intrusos se basa en el análisis del tráfico de red y normalmente se integra con un firewall, ya que el IDS es incapaz de detener los ataques por si solo excepto cuando trabaja conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall. El sistema de detección de intruso evaluara una intrusión cuando esta tenga lugar y generara una alarma, mientras que el firewall limitara el acceso a redes para así prevenir la intrusión pero teniendo en cuenta que una vez que se salta el firewall, este es incapaz de analizar lo que ocurre internamente en la red. Por lo tanto el uso combinado se convertirá en una poderosa herramienta que unirá el poder de bloqueo del firewall al análisis del sistema del IDS. (Castillo, 2019)

El funcionamiento se lo puede definir como un proceso de auditoría de la información del sistema de la red o de un computador, logrando a través de un configuración y de una base de datos “firmas” prevenir y detectar posibles ataques de intrusos.

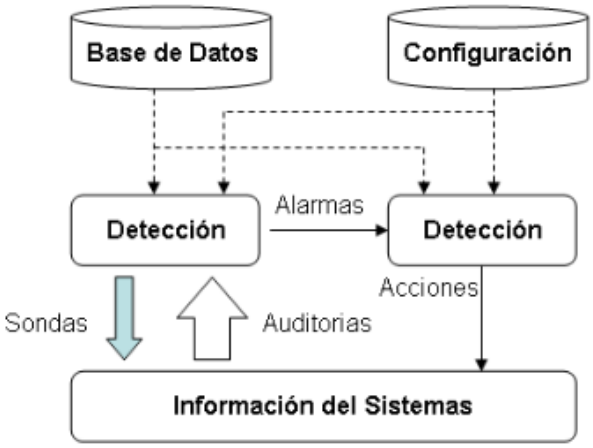


Ilustración 1. Funcionamiento de los IDS (Lopez M. , 2017)

El proceso de detección de intrusos, se lo define de la siguiente manera:

- Una base de datos con una recopilación de ataques anteriores.
- Un sistema actual debidamente configurado.

- Estado actual, referente en términos de comunicación y procesos.

Los atacantes pueden adoptar diferentes enfoques cuando intentan penetrar en un sistema. Con el software de detección de intrusos en la red, comprender que tipos de ataques se pueden usar es de vital importancia para establecer una prevención efectiva. En muchos casos de intrusión en la red, el ataque implica inundar o sobrecargar la red, recopilar datos sobre la red para atacarla desde un punto débil más tarde o insertar información en la red para propagarse y obtener acceso desde adentro. Estos son algunos de los tipos comunes de intrusión y ataque de red:

- Escaneo de ataque
- Enrutamiento asimétrico
- Ataques de desbordamiento de búfer
- Ataques específicos de protocolo
- Malware
- Inundaciones de trafico

Ventajas y Desventajas de un sistema de detección de intrusos

El sistema de detección de intrusos cuenta con ventajas y desventajas que deben conocerse, puesto que permitirán complementar este sistema de seguridad con otras soluciones, para hacer más resistente todo el sistema.

Entre las ventajas de un sistema de detección de intrusos están:

- Permite identificar incidentes de seguridad gracias al registro que hace de ellos.
- Puede ayudar a identificar problemas o errores de seguridad en la red o en los dispositivos.
- Permite el monitoreo de la red y de los dispositivos en tiempo real.

- Puede ayudar a automatizar nuevos patrones de búsqueda de amenazas en los paquetes de datos enviados de la red.
- Ayuda con el cumplimiento normativo en materia de ciberseguridad y seguridad de la información.

  Mientras que sus principales desventajas son:

  - No pueden prevenir o bloquear ataques, ya que su función es reactiva y no proactiva.
  - Son vulnerables a ataques DDoS, puesto que pueden causar que el IDS deje de funcionar.
  - Pueden dar falsos positivos.

Sistemas de Detección de Intrusos Plataforma Open Source

Dentro de la investigación se tomó en cuenta los siguientes sistemas de detección de intrusos basados en la plataforma Open Source: Snort y Suricata.

Snort

Snort es un sistema de detección de intrusos (IDS) basado en red (NIDS) Open Source que está escrito en lenguaje de programación C. Fue desarrollado en 1998 por Martin Roesch. Ahora está desarrollado por Cisco. Cuenta con un lenguaje de creación de reglas en el que se pueden definir los patrones que se utilizaran a la hora de monitorizar el sistema. Además ofrece una serie de reglas y filtros ya predefinidos que se pueden ajustar durante su instalación y configuración para que así se adapte lo máximo posible a lo que se desee, su última versión es Snort 3.0, puede ser configurado a modo de sniffer, packet logger y NIDS. (Snort, 2022)

Se basa en la herramienta de captura de paquetes de la biblioteca. Las reglas son bastante fáciles de crear e implementar y se pueden implementar en cualquier tipo de sistemas

operativo y cualquier tipo de entorno de red. Snort es un sistema de detección de intrusiones en la red, pero viene con tres modos de operación, cabe señalar que cada uno de estos modos tiene varias opciones que se pueden configurar a través de parámetros de líneas de comando o incluso archivos de configuración.

Características de Snort

Estas son las principales características de Snort:

- Monitor de tráfico en tiempo real
- Registro de paquetes
- Análisis de protocolo
- Coincidencia de contenido
- Huellas digitales del SO
- Puede instalarse en cualquier entorno de red
- Fuente abierta
- Las reglas son fáciles de implementar.

Suricata

Suricata es un motor de red de alto rendimiento IDS, IPS y seguridad de red, desarrollado por el OISF, esta es una aplicación de código abierto multiplataforma y es propiedad de una fundación sin ánimo de lucro de la comunidad Open Information Security Foundation (OISF). (Candel, 2021)Esta es una herramienta escalable, este monitor de seguridad hace uso de las funciones multi-hilo de manera que solo con ejecutarse en una instancia el monitor balanceara su carga entre todos los procesadores disponibles, evitando

incluso alguno de ellos si así se lo específica, gracias a ello esta herramienta es capaz de procesar un ancho de banda de hasta 10 gigabits por segundo sin que ellos repercuta sobre el rendimiento. (Pérez, 2020)

Está basado en un conjunto de reglas desarrolladas externamente para supervisar el tráfico de la red y proporcionar alertas al administrador del sistema cuando se producen eventos sospechosos. Diseñada para ser compatible con los componentes de seguridad de red existentes, ofrece funcionalidad de salida unificada y opciones de biblioteca. Como un motor de múltiples hilos, ofrece una mayor velocidad y eficiencia en el análisis de tráfico de red. Actualmente se encuentra en su versión 4.0 con mejoras en las capacidades de detección de intrusos y también en el soporte de más protocolos y opciones, mejorando en el motor de flujo TCP y su IDS.

Características de Suricata

Entre las características de Suricata se encuentran las siguientes:

- Multi-threading
- Soporte GPU
- Estadística de Rendimiento
- Fast IP Matching
- IP Reputation, GeoIP, IP list support
- Graphic Cards Acceleration
- Soporta Lua Scripting
- Detección automática de protocolos
- Inspección y registro de peticiones de varios protocolos como HTTP, DNS, TSL/SSl.
- Inspección del tráfico de red empleando tanto reglas configurables como reglas ya predefinidas para detectar amenazas y comportamientos sospechosos.

Sistemas de Detección de Intrusos Plataforma Software Propietario

Para la investigación se tomó en cuenta los siguientes sistemas de detección de intrusos basados en la plataforma Software propietario: Nessus y Atomic OSSEC.

Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema operativo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. La operación de Nessus comienza escaneando los puertos con map o con su propio escaneador de puertos para buscar puertos abiertos y después intentar exploits para atacarlo. El proyecto Nessus comenzó en 1998, cuando Renaud Deraison quiso que la comunidad de internet tuviese un escáner remoto de seguridad que fuese libre aunque hoy en día su licencia ha cambiado se ha convertido en software propietario. (Caswell, 2015)

Características de Nessus

Estas son algunas de las características de Nessus:

- Escaneo de alta precisión con bajo número de falsos positivos
- Genera archivos
- Escalabilidad a ciertos de miles de sistemas
- La interfaz gráfica de usuario (GUI) muestra resultados en tiempo real
- Brinda una interfaz unificada para el analizador

- Los análisis se ejecutan en el servidor, aun así se lo desconecte
- Los informes de los análisis de Nessus pueden cargarse.
- Implementación y mantenimiento sencillos
- Bajo costo de administración y operación

Atomic OSSEC

Atomic OSSEC es un sistema de software de protección de cargas de trabajo en la nube y de punto final que aprovecha la naturaleza rápida de la operación de seguridad de código abierto para cumplir con todos los requisitos de detección y respuestas extendidas (XDR). Estos requisitos incluyen capacidades de seguridad más profundas y avanzadas que los sistemas de detección y respuesta de puntos finales (EDR) y los sistemas de detección de intrusos (IDS) de generaciones anteriores. Atomic OSSEC es la oferta comercial de detección de intrusos basado en OSSEC de Atomicorp que brinda toda la protección avanzada de un sistema de detección y respuesta extendida (XDR). (Vora, 2017)

Atomic OSEEC proporciona detección de intrusiones, monitoreo de integridad de archivos, administración de registros, informes de cumplimiento, escaneo de vulnerabilidades, respuesta activa, además que puede realizar una detección de intrusiones de alta fidelidad en cientos de sistemas operativos, aplicaciones y servicios. Realiza un análisis de vulnerabilidades basado en host en Windows, RedHat, Centos, Debian y Ubuntu.

Características de Atomic OSSEC

Estas son algunas de sus características:

- Detección de intrusiones basados en host,
- Funciona con la mayoría de los sistemas operativos
- Soporte técnico experto
- Análisis de vulnerabilidades
- Alertas y notificaciones
- Administrador de reglas
- Soporte desarrollado en reglas
- Sistema de alertas y análisis de logstash

Metodología de la Investigación

El presente caso de estudio se lo realizo utilizando la investigación descriptiva porque de esta manera se identifica las características, importancia, funcionalidad y los beneficios acerca del tema de investigación.

Dado que uno de los objetivos es determinar las características y funcionalidades de los diferentes sistemas de detección de intrusos, se implementó este tipo de investigación ya que de esta manera facilita enfocarse en los diferentes aspectos de los tipos de sistemas de detección de intrusos.

Método Cualitativo

El presente caso de estudio fue diseñado bajo el planteamiento metodológico del enfoque cualitativo, debido a que en el cumplimiento de los objetivos planteados de la investigación es el que se adapta mejor a las características y necesidades. Además en este método se realiza un análisis de texto y la comparación entre los diferentes conceptualizaciones encontradas en la investigación.

Técnica de recolección de datos

La técnica de recolección de datos que se implementó para la realización de esta investigación en el análisis documental y bibliográfico porque este proceso buscar reunir información de diferentes fuentes para obtener una visualización completa y precisa acerca del tema de investigación y además que permite analizar datos cualitativos de forma sencilla para comprender la información obtenida.

Análisis comparativo entre Sistemas de detección de intrusos Open Source y Software propietario.

Para realizar la comparación de los diferentes sistemas de detección de intrusos se han tomado en cuenta las características principales de cada uno de ellos.

Parámetros	**Open Source**		**Software Propietario**	
	Snort	**Suricata**	**Nessus**	**Atomic OSSEC**
Compatibilidad	Linux, Windows macOS / MacOS X.	Linux, FreeBsd, OpenBSD, macOS / Mac OS X Windows.	Linux, FreeBsd, OpenBSD, macOS / Mac OS X Windows Solaris, Ubuntu.	Linux, FreeBsd, OpenBSD, macOS / Mac OS X Windows.
Free Trial	Software libre	Software libre	Si	Si
Multi-Threading	No	Si	No	No
Detección automática de protocolos	No	Si	Si	Si

Aceleración de GNU	No	Si	Si	Si
Aceleración con GPU	No	Si	Si	Si
Detección de alertas basada en reglas	Si	Si	Si	No
Detección de alertas basada en scripts	No	No	Si	Si
Soporte para IPV6 / IPV4	Si	Si	Si	Si
IP Reputación	No	Si	Si	si
Variables globales/Flowbits	No	Si	Si	Si
GeoIP	No	Si	Si	Si
Análisis avanzado de HTTP	No	Si	Si	Si
HTTP Access Logging	No	Si	Si	Si

Tabla 1 Tabla comparativa de los IDS Open Source y Software propietario
Elaborado por: Jenny Castillo

En relación a la comparativa entre los sistemas de detección de intrusos podemos decir que Suricata, Nessus y Atomic OSSEC cuenta con muchos parámetros que ayuda a detectar intrusiones y resguardar la seguridad de los sistemas o redes, mientras que Snort no cuenta con algunos parámetros aunque igual es un IDS que tiene muchas ventajas, en resumen se puede ver que los sistemas de detección de intrusos Open Source y Software propietario tienen algunas similitudes en sus características.

Aunque Snort y Suricata están basados en firmas o reglas y su funcionalidad se basa en el conocimiento sobre malware y utilizan el mismo conjunto de reglas; por otro lado Nessus es un analizador de seguridad de redes potente, con una amplia base de datos de plugins que se actualiza a diario, además consiste en daemon, llamado “nessusd”, que realiza

el escaneo en el sistema objetivo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos y por ultimo Atomic OSSEC tiene como cometido analizar los registros de eventos del sistema operativo, reglas de alerta personalizadas y escritura de reglas de acción en respuesta a las alertas de seguridad.

CONCLUSIONES

Los Sistemas de Detección de Intrusos (IDS) tienen funcionamientos y características diferentes sea de plataforma Open Source o Software Propietario, a pesar de sus diferencias tienen algo en común que es detectar accesos no autorizados a un ordenador o red, emiten una alerta oportuna, estos sistemas permiten ver lo que está sucediendo en la red en tiempo real, recopila y analiza la información desde un sistema o red

Las características de los Sistemas de detección de intruso de plataforma Open Source, Snort y Suricata proporcionan un mayor rendimiento, escalabilidad, usabilidad y permiten una gran extensibilidad, poseen sus propias reglas, son fáciles de usar y su principal razón de popularidad es porque son software gratuitos y de código abierto, por lo que cualquier usuario o empresa puede usarlo.

Los Sistemas de detección de intrusos de Software propietario es decir, Nessus y Atomic OSSEC se destacan por el diseño y la innovación de sus funciones para cubrir las

necesidades de diferentes usuarios y/o empresas. Son sistemas fáciles de usar, brindan soluciones óptimas, amplían las capacidades de lo que las empresas necesiten y proporcionan seguridad de los datos.

Mediante la presente investigación se pudo concluir que ambas plataformas de sistemas de detección de intrusos son muy útiles para la detección de intrusos, pero realmente no hay un sistema mejor o peor, realmente depende de lo que esté buscando el usuario o empresa y de que sistema llena mejor los vacíos en la detección de intrusos.

Bibliografía

Asociación de Gestión, R. d. (2019). *Seguridad en la Nube: Conceptos, Metodologías, Herramientas y Aplicaciones.* IGI Global.

Atico, G. (2021). *Protecciondatos*. Obtenido de Protecciondatos: https://protecciondatos-lopd.com/empresas/sistema-deteccion-intrusiones-ids/

Briceño, E. V. (2021). *Seguridad de la Informacion .* 3Ciencias.

Candel, O. (2021). *Ciberseguridad, Manual práctico.* Editorial Paraninfo.

Castillo, C. d. (2019). *Sistemas IDS.* CEP.

Caswell, B. (2015). *Nessus, Snort y Ethereal Power Tools.* Elsevier.

Lopez, J. G. (2015). *Optimizacion de Sistemas de deteccion de intrusos en red utilizando tecnicas computacionales avanzadas.* Universidad Almeria.

Lopez, M. (10 de Julio de 2017). *Cybsec*. Obtenido de Cybsec: http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf

Miranda, V. (2014). *Redes Telematicas.* Paraninfo.

Pérez, G. M. (2020). *Security in Computing and Communications.* Springer Nature.

Snort. (2022). *Snort*. Obtenido de Snort: https://www.snort.org/snort3

Vora, Z. (2017). *Enterprise Cloud Security and Governance.* Packt Publishing Ltd.

Zorrilla, R. E. (2020). *Ciberseguridad sin Destinatario: La Ciberseguridad no es una moda.*

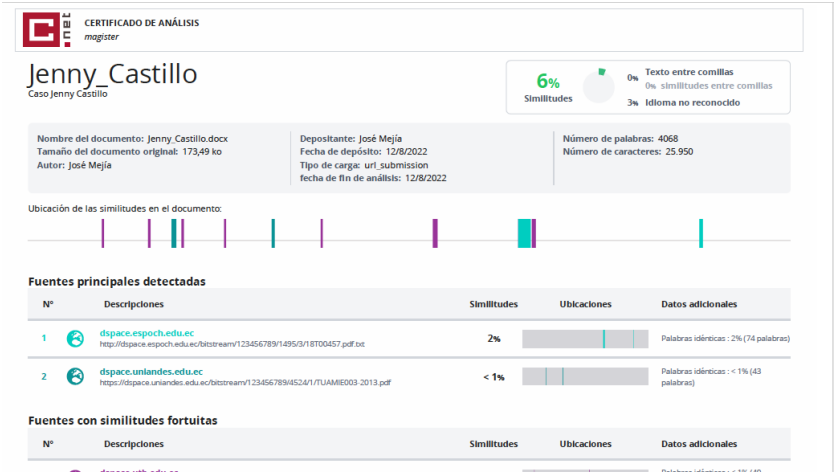
ANEXO

Babahoyo, 11 de agosto del 2022

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación del Srta: Castillo Mendoza Jenny Isabel, cuyo tema es: Análisis de los Sistemas de detección. de intrusos(IDS) open source y software Propietario, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio obteniendo como porcentaje de similitud de [6%], resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



CERTIFICADO DE ANÁLISIS
magister

Jenny_Castillo
Caso Jenny Castillo

6% Similitudes
0% Texto entre comillas
0% similitudes entre comillas
3% Idioma no reconocido

Nombre del documento: Jenny_Castillo.docx
Tamaño del documento original: 173,49 ko
Autor: José Mejía

Depositante: José Mejía
Fecha de depósito: 12/8/2022
Tipo de carga: url_submission
fecha de fin de análisis: 12/8/2022

Número de palabras: 4068
Número de caracteres: 25.950

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.espoch.edu.ec http://dspace.espoch.edu.ec/bitstream/123456789/1495/3/18T00457.pdf.txt	2%		Palabras idénticas : 2% (74 palabras)
2	dspace.uniandes.edu.ec https://dspace.uniandes.edu.ec/bitstream/123456789/4524/1/TUAMIE003-2013.pdf	< 1%		Palabras idénticas : < 1% (43 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

_____

Ing.Sist. José mejía Viteri, MSc.
DOCENTE DE LA FAFI.